What is claimed is:

1. A method for filtering packets, comprising:
receiving a packet sent from a first device to a second device;
authenticating an identifier for said packet;
determining whether to send said packet to said second device; and
sending said packet to said second device in accordance with said determination.

2. The method of claim 1, wherein said determining comprises:
comparing said identifier to a list of identifiers;
retrieving at least one policy rule;
determining whether to send said packet to said second device in accordance with said comparison and said policy rule.

3. The method of claim 1, wherein said identifier is a common host identifier.

4. The method of claim 1, wherein said authenticating is performed in accordance with IPSEC standards.

5. The method of claim 1, wherein said authenticating comprises:
retrieving a pointer to a security association from an authentication header from said packet;
retrieving a key associated with said security association; and
determining whether said packet is authentic using said key.

6. The method of claim 5, wherein said identifier is not authentic, further comprising sending a first message to a third device indicating said identifier is not authentic.

7. The method of claim 5, wherein said authentication header is an IPSEC authentication header.

8. The method of claim 1, wherein said packet is encrypted prior to said receiving, further comprising decrypting said packet prior to authenticating.

9. The method of claim 8, wherein said packet is encrypted and decrypted using one of group of cryptographic techniques comprising DES, triple DES, HMAC and RSA.

10. The method of claim 1, wherein said policy rule is stored in a policy configuration file at said second device.

11. A machine-readable memory whose contents cause a computer system to perform packet filtering, by performing the steps of:

receiving a packet sent from a first device to a second device;

authenticating an identifier for said packet;

determining whether to send said packet to said second device; and

sending said packet to said second device in accordance with said determination.

12. The machine-readable memory of claim 11, wherein said determining comprises:

comparing said identifier to a list of identifiers;

retrieving at least one policy rule;

determining whether to send said packet to said second device in accordance with said comparison and said policy rule.

13. The machine-readable memory of claim 11, wherein said identifier is a common host identifier.

14. The machine-readable memory of claim 11, wherein said authenticating is performed in accordance with IPSEC standards.

15. The machine-readable memory of claim 11, wherein said authenticating comprises:

retrieving a pointer to a security association from an authentication header from said packet;

retrieving a key associated with said security association; and

determining whether said packet is authentic using said key.

16. The machine-readable memory of claim 15, wherein said identifier is not authentic, further comprising sending a first message to a third device indicating said identifier is not authentic.

17. The machine-readable memory of claim 15, wherein said authentication header is an IPSEC authentication header.

18. The machine-readable memory of claim 11, wherein said packet is encrypted prior to said receiving, further comprising decrypting said packet prior to authenticating.

19. The machine-readable memory of claim 18, encrypted and decrypted using one of group of cryptographic techniques comprising DES, triple DES, HMAC and RSA.

20. The machine-readable memory of claim 11, wherein said policy rule is stored in a policy configuration file at said second device.

21. A packet filter for a distributed firewall, comprising:

an input means coupled to said first network for receiving a data packet from a first device, said data packet having an encrypted common host identifier;

a first buffer coupled to said input means for storing said received packet;

a first memory segment containing a list of common host identifiers and at least one policy rule;

a second memory segment for storing a program for decrypting said common host identifier, authenticating said common host identifier, and determining whether to send said packet to a second device based on said list and said policy rule;

a processor coupled to said first buffer, said first memory segment and said second memory segment for executing said program; and

an output means coupled to said first buffer for forwarding said compared data packet to said second device based on said comparison.

22. The apparatus of claim 1, further comprising a second buffer for storing said compared data packet prior to forwarding said compared data packet to the second device.

23. The apparatus of claim 22, wherein said random access memory comprises dynamic random access memory.

24. The apparatus of claim 23, further comprising a non-volatile random access memory for storing parameters used by said operating system program.

25. The apparatus of claim 24, further comprising means for receiving an updated list of origination addresses.

26. The apparatus of claim 25, wherein said means for receiving comprises an asynchronous terminal device and a serial port coupled to said dynamic random access memory.

27. The apparatus of claim 25, wherein said means for receiving comprises a network interface card coupled to said dynamic random access memory.

28. The apparatus of claim 21, wherein said first network is a wireless network, and said input means comprises means for receiving said data packets from said wireless network.

29. A distributed firewall system, comprising:

a first network device;

a second network device in communication with said first network device;

a packet filter processor for each network device;

an encryption means coupled to said packet filter processor, said encryption means for decrypting and authenticating a packet sent between said first network device and said second network device; and

a system management module to manage said packet filter processors.